Motorola Solutions

SCADA Security

Tom Rigsbee PE

US Federal Government Markets

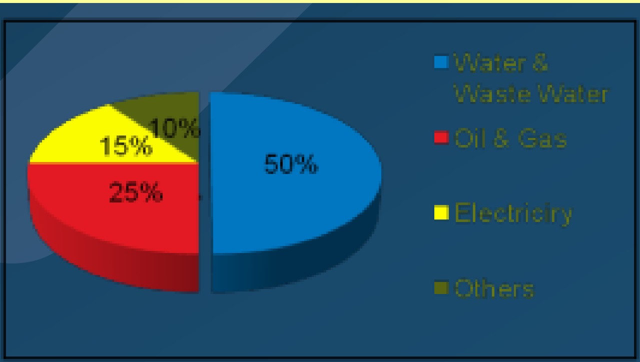
April 2012

Motorola SCADA & Irrigation - Background

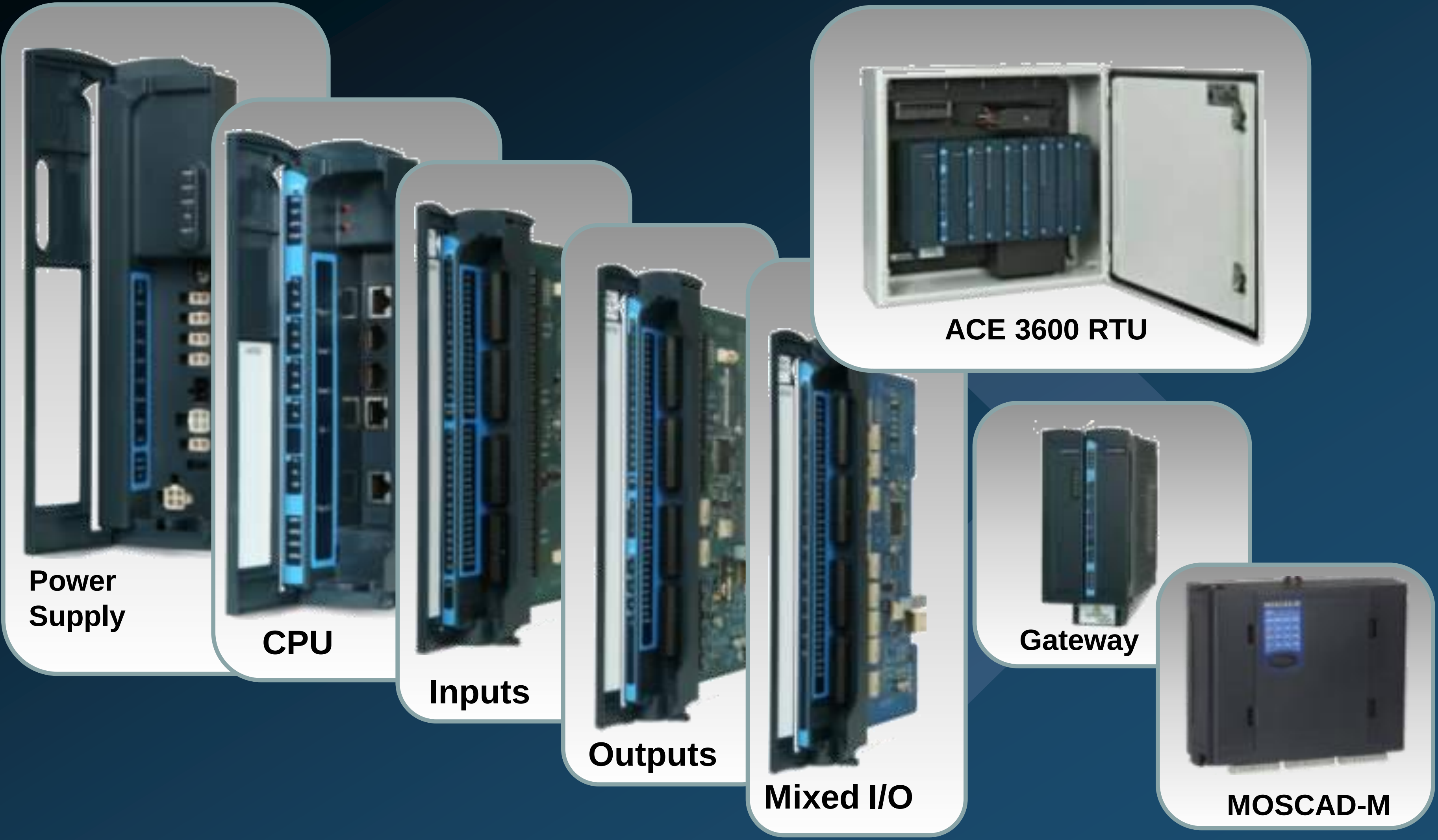
- Motorola is in the SCADA business ~40 years
- Install base of over 200,000 units all over the world
- SCADA sales mainly via the indirect sale channels (VARs):
  - NAG: 45 SCADA VARs
  - EMEA, APAC, LA: 50 SCADA VARs
- Large wireless install base – can use P25 radio IV&D system

SCADA Markets

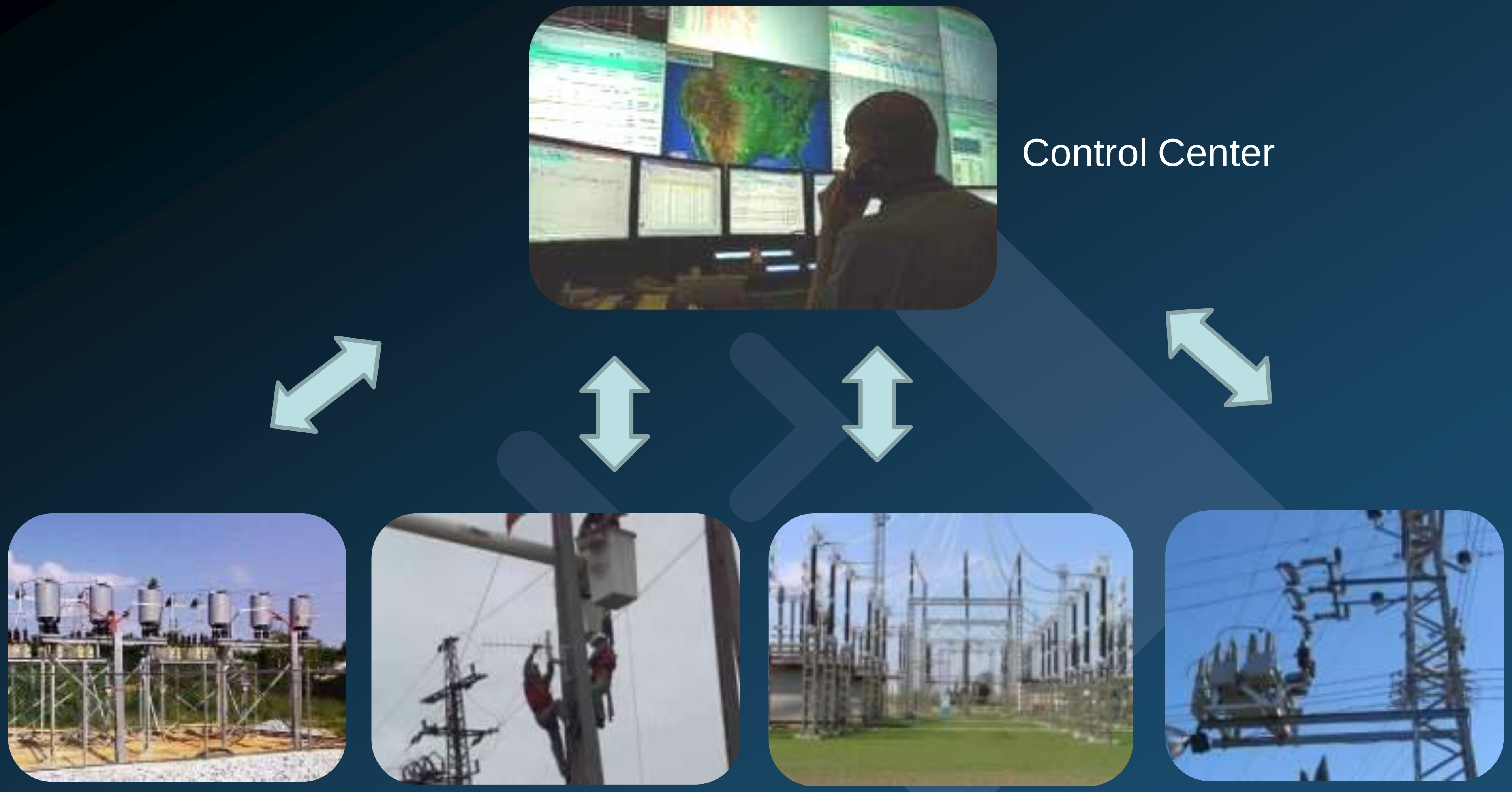
- Water Distribution Systems
- Waste Water Systems
- Electric Power Distribution Systems
- Oil and Gas Production / Pipelines
- Early Warning Systems
- Irrigation and Water Management Systems
- Transportation Systems
- Environmental Monitoring
- Communication Systems



SCADA RTU - Products Portfolio



Electric Power Distribution



Control Center

Capacitor Bank Control

Fault Detection

Substation Control

MV Line Switching

Typical Distribution Automation Installations

Mechanical Air Break Switch Control

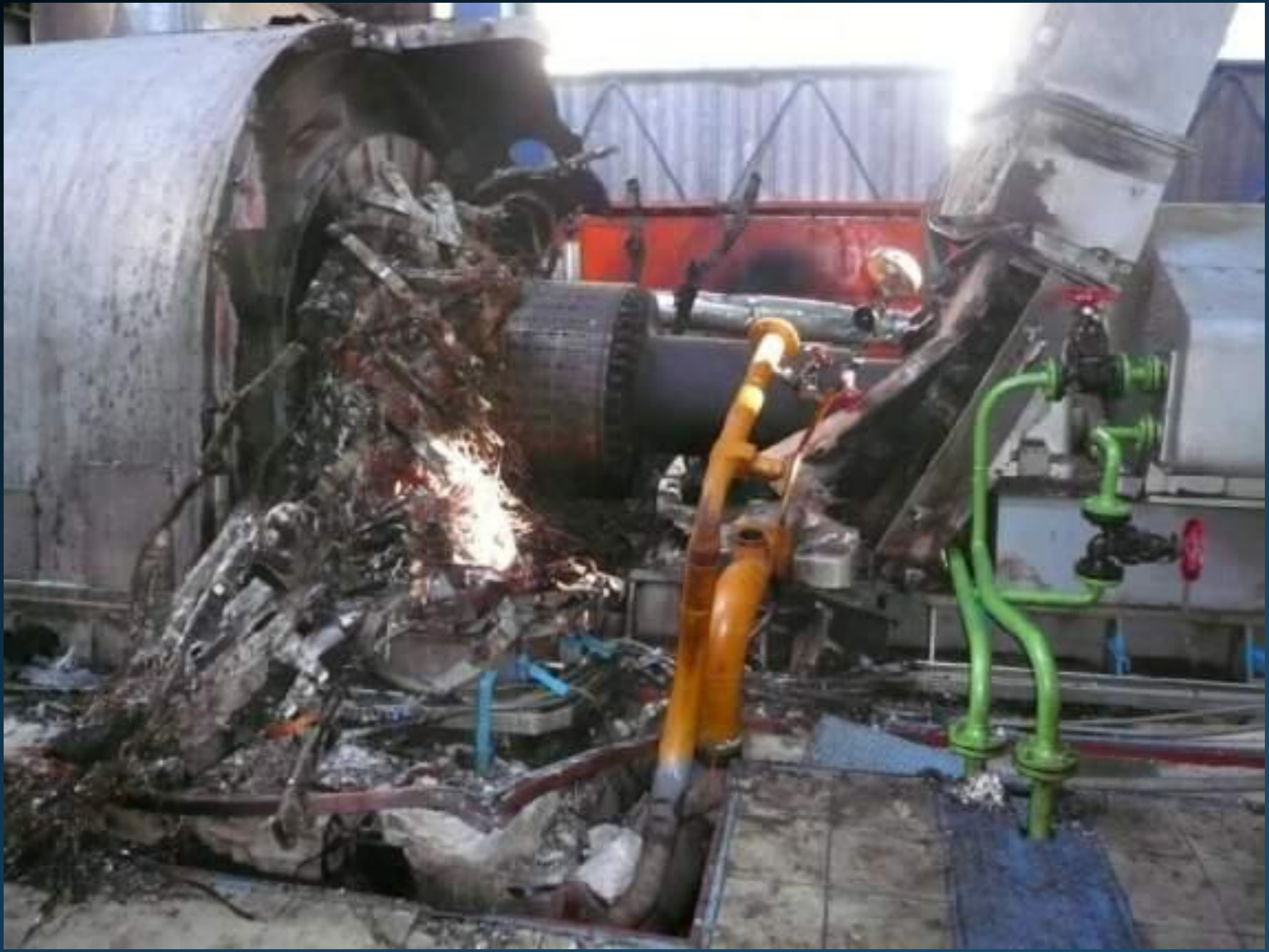
Medium Voltage SF–6 Switches

SCADA & Controlled Systems Attacks

A Good Day at a Natural Gas Turbine Generator Station

Unauthorized review, use or copy or disclosure or distribution is prohibited

A Bad Day at Iranshahr Power Plant



خطر
DANGER

SCADA & Controlled Systems Attacks

ACE 3600 System Security Policy

- ACE 3600 Advanced Security provides **a system-wide security policy** enforcement solution.

- ACE 3600 Security Policy is a set of configurable system-wide security parameters for enforcing the organization’s security policy in the ACE 3600 system management tools (STS), front-end units and field units.

User Accounts

- To ensure system integrity, a User Account is required to access any part of the ACE 3600 secured system, including management tools (STS), front-end units and field units.

- User Access is gained by a **unique** User Name and User Password.

- User Accounts are managed by system administrators.

User Authentication

- Users credentials are authenticated by the ACE 3600 Authentication Server.
- Per security policy definition, users credentials can also be authenticated locally by the field units.
- The system administrators can enable/disable user access indefinitely or for specific time periods, and for specific field units.

Role Based Permissions

- Usage of roles to restrict access of authorized users.
- Roles are created by an administrator per various organizational job functions.
- Permissions to perform certain operations in the system are assigned to specific roles.

Field Unit Authentication

- To ensure system integrity, a field unit receiving a message from another unit, authenticates the Machine-to-Machine ("M2M") credentials of the sending unit.

Communications Encryption

- ACE 3600 MDLC protocol enables data communications over a wide range of communications media, such as telephone lines, radio, IP networks, cellular networks, etc.
- MDLC *enhanced* encryption seamlessly secures the communications over any communication media.
- MDLC data encryption with a FIPS-140-2 approved AES 256 encryption algorithm.

Encryption Key Management

- ACE 3600 management tools provide an efficient Key Management facility to the system administrators.
- The Key Management facility enables generation, distribution, storage, safeguarding, and tracking of the encryption keys in the system.
- A group of keys can be downloaded to the units. Key replacement in the units is automatic upon the key expiration date.

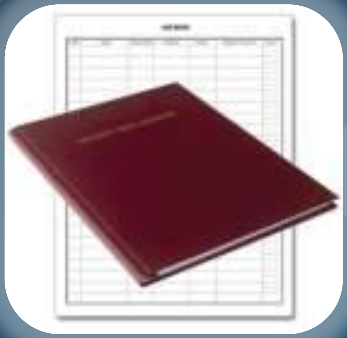
- The new key and the previous key are both valid for a pre-defined time period after key replacement.

Data File Encryption

- A ‘local data’ encryption key is stored safely in the unit and is not visible to anyone (including the administrators.)
- Sensitive data files can be encrypted on the field units and in the management tools using a FIPS-140-2 approved AES 256 encryption.

Security Log

- The ACE 3600 field units and management tools keep an encrypted local Security Log that contains records of access activity and other security-related events.
- Events are logged with essential data such as user name, time & date, description and event severity.
- Alerts can be sent from the ACE 3600 units to the control center upon logging of high severity events.



IP Firewall

- Protects the field units from unauthorized TCP and UDP packet access while permitting legitimate packets to pass.
- The administrators can specify the list of IP addresses to accept, i.e. the list of IP addresses allowed to pass through this firewall.

Run-files White Listing

- Run-files (user program application) loaded to the RTU from the STS by an authorized user will be "white listed" by the RTU.

- The RTU will run only a "white listed" file which was not modified since it was "white listed".

- The RTU will not run a file which:
  - **Is not "white listed"**
    or
  - **Seems to have changed since it was "white listed".**

- Detection of tampered "white listed" files will be logged in the security log and alerted.

Secured Programming and Port Scanning

- Secured coding methodologies are employed in the development process to prevent defects, bugs and logic flaws which might cause commonly exploited software vulnerabilities.
- Auxiliary data related to debugging and testing which might be exploited is eliminated or encrypted.
- IP ports are scanned to detect, assess and correct any security vulnerabilities that are found.

Enhanced Security Features

- **The main security features are** :
  - User access authentication by user name and password
  - Role based permissions
  - Communication encryption (AES 256)
  - Data files encryption (AES 256)
  - Run files whitelisting
  - IP firewall
  - Remote STS access blocking
  - Security log for audit
  - Security Management (system security policy, user management, key management, etc)
  - Secured programming methods

THANK YOU